REMARKS

Claims 1-34 are pending in the present application.

In the office action mailed July 8, 2005 (the "Office Action"), claims 1-34 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,810,525 to Safadi *et al.* (the "Safadi patent").

The "impulse pay-per-use" ("IPPU") system of the Safadi patent was described in detail the response previously filed on April 19, 2005 (the "previous response"). In summary, the Safadi patent describes a secure IPPU system where a request for a subscriber IPPU selection made from a subscriber terminal 16 is provided to an access controller 14 or a customer response center (CRC)/billing system 12. *See* col. 5, lines 1-5; col. 5, lines 33-48. The IPPU selection is processed by the access controller 14 or the billing system 12 and provides an encrypted message back together with the cost of the IPPU service to the subscriber terminal 16. *See* col. 5, lines 5-12. Upon verification of the cost of the IPPU service, an encrypted entitlement token is securely provided to a server 18. The entitlement token is generated by a secure processor at the subscriber terminal 16 or generated by the access controller 14 and provided to the subscriber terminal 16 to be forwarded onto the server 18. *See* col. 5, lines 13-21. The server 18 uses the entitlement token to determine entitlement to the requested IPPU selection. *See* col. 5, lines 21-24. Once the entitlement to the requested IPPU selection is verified, content associated with the IPPU selection is forwarded by the server 18 to the subscriber terminal 16. *See* col. 5, lines 24-26.

Claims 1, 11, 19, 27, and 31 are patentably distinct from the Safadi patent because the Safadi patent does not disclose the combination of limitations recited in the respective claim.

For example, with respect to claim 1, the Safadi patent fails to at least disclose a method for providing access to computer resources on a computer system including, among other things, decrypting at the computer system a token under control of a remote application manager component on the computer system. As previously discussed, the subscriber terminal 16 securely forwards an encrypted entitlement token to a server 18 for fulfillment. The subscriber terminal 16 does not decrypt the entitlement token. Even in the case where the entitlement token is generated by the access controller 14 and then provided to the subscriber terminal 16, the token is merely forwarded onto the server 18 and is never decrypted by the subscriber terminal 16. As described in the Safadi patent, the purpose of the encrypted entitlement token is

for verifying the subscriber's entitlement to the requested IPPU selection. That is, there is no need for the subscriber terminal 16 to ever decrypt the token, and consequently, it never does.

As discussed in the previous response, the material cited by the Examiner, namely col. 2, lines 47-55 of the Safadi patent, as disclosing the limitation of "under control of the remote application manager component, decrypting the token and authenticating a user of the computer system using authentication information stored in the token," *see* the Office Action at page 3, merely discloses an alternative embodiment where a *signed* and encrypted entitlement token is securely sent from the client application to the server for authentication and decryption. *See* col. 2, lines 47-55. As the cited material clearly indicates, the server decrypts the entitlement token and not the subscriber terminal 16. This is in contrast to the method recited in claim 1, which recites that the token is decrypted *at the computer system* under the control of the remote application manager, the computer system authenticated using authentication information stored in the token (*e.g.*, processor identification number of the processor in the computer system). As described in the Safadi patent, it is desirable for the server 18 to have a secure mechanism to determine whether the subscriber is legitimately entitled to the requested IPPU services. *See* col. 4, lines 50-59. This material suggests that it preferable for the entitlement token to not only be encrypted, but to also be securely transferred to the server 18. As part of the "secure" transfer mechanism, the entitlement token is forwarded to the server 18 in an encrypted format. As such, decryption of the entitlement token by the subscriber terminal 16 is undesirable.

Claims 11, 19, and 27 include similar limitations as claim 1 that distinguish the respective claimed invention from the Safadi patent. Claim 11 recites in pertinent part a method for providing access to computer resources on a computer system including, under control of a remote application manager component on a client system, decrypting at the client system the token in response to a request to initiate execution of one of the computer resources. Claim 19 recites in pertinent part a method for providing access to computer resources on a computer system including client and server systems including, under control of the remote application manager component on the client system, decrypting at the client system a token including encrypted information. Claim 27 recites in pertinent part a client system for providing access to computer resources including a remote application manager component adapted to receive encrypted user information contained in the token, the remote application manager operable

responsive to a request to open a computer resource component to decrypt at the client system the encrypted user information.

As previously discussed with respect to claim 1, the Safadi patent does not disclose decrypting the entitlement token by the subscriber terminal 16. The encrypted entitlement token is securely provided to the server 18 for verification of the subscriber's entitlement to the subscriber requested IPPU content. The Safadi patent acknowledges the need for a secure mechanism between the access controller 14, the subscriber terminal 16, and the server 18 in order to determine whether the subscriber is legitimately entitled to the requested content. As part of the solution described in the Safadi patent to meet this requirement, the subscriber terminal 16 forwards the entitlement token to the server 18 for decryption, rather than the subscriber terminal 16 every decrypting it and then forwarding the same information to the server 18.

As for claim 31, the Safadi patent fails to at least disclose a server system having a token generation component and a computer resource component including a plurality of computer resources to be transferred to client computers. As previously discussed, the Safadi patent describes generating the encrypted entitlement token at either the subscriber terminal 16 by way of a secure processor or generating the entitlement token at the access controller 14 and then providing the token to the subscriber terminal 16. The entitlement token is received and decrypted by the server 18 verification of the subscriber's entitlement to the requested IPPU content. The server 18 does not generate an entitlement token.

For the foregoing reasons, claims 1, 11, 19, 27, and 31 are patentably distinct from the Safadi patent. Claims 2-10, which depend from claim 1, claims 12-18, which depend from claim 11, claims 20-26, which depend from claim 19, claims 28-30, which depend from claim 27, and claims 32-34, which depend from claim 31 are similarly patentably distinct from the Safadi patent because of their dependency from a respective allowable base claim. Therefore, the rejection of claims 1-34 under 35 U.S.C. 102(e) should be withdrawn.

All of the claims pending in the present application are in condition for allowance. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,

DORSEY & WHITNEY LLP

Marcus Simon
Registration No. 50,258
Telephone No. (206) 903-8787

MS:ajs

Enclosures:
Postcard
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, Washington 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\clients\micron technology\700\500767.01\500767.01 amend after final reject 1.116.doc